

FILED

SEP 20 2024

Clerk, US District Court
District of Montana - Billings

IN THE UNITED STATES DISTRICT COURT
FOR MONTANA

IN THE MATTER OF THE SEARCH OF
BLACK SAMSUNG CELL PHONE TAKEN
FROM WARREN JONES CRAZYBULL

MJ-24-124-BLG-TJC

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, **JERRARD CARTER**, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Senior Special Agent with the United States Secret Service (USSS) and have been since July 16, 2001. In 2001, I attended the Criminal Investigator Training Program at the Federal Law Enforcement Training Center (FLETC). This training covered the investigation of violations of federal laws, the process of criminal investigations, and the judicial process. Following FLETC, I attended the Secret Service training academy in Beltsville, Maryland (MD). This training focused specifically on violations of federal laws that the Secret Service investigates; to include bank fraud, access device fraud, wire fraud, crimes relating to counterfeit currency, cyber-crimes, and protective intelligence. During my training at the FLETC and the Secret Service Academy, I received instruction how electronic devices, including the use of cell phones, electronic media, social media, and optical media storage devices are used in various types of violation of federal laws, or to store evidence of said violations. Agents are vigorously

trained in protective intelligence, more commonly known as “threat cases” related to violations of Title 18, United States Code, Sections 871, 878, and 879.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Rather the information contained in this affidavit is based on my personal knowledge, as well as the knowledge and investigative information provided to me by other law enforcement agents and witnesses, interviews, and my personal examination of reports, and records. This affidavit only contains those facts and circumstances necessary to establish probable cause to search the identified electronic device and does not include each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause for a Search Warrant.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is a black Samsung cellphone, serial number/IMEI 353122990895992, hereinafter the “Device.” The Device is currently located in the possession of the USSS Billings, MT Resident Agency.

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

APPLICABLE STATUTE

6. Title 18, United States Code, Section 879(a)(1) states:

(a) Whoever knowingly and willfully threatens to kill, kidnap, or inflict bodily harm upon—

(1) a former President or a member of the immediate family of a former President;

shall be fined under this title or imprisoned not more than 5 years, or both.

PROCEDURES FOR ELECTRONICALLY STORED INFORMATION AND FORENSIC ANALYSIS

7. It is not possible to determine, merely by knowing the cellular telephone's make, model, and serial number, the nature and types of services to which the device is subscribed and the nature of the data stored on the device. Cellular devices today can be simple cellular telephones and text message devices, can include cameras, can serve as personal digital assistants, and have functions, such as calendars and full address books and can be mini-computers allowing for electronic mail services, web services and rudimentary word processing. An increasing number of cellular service providers now allow for their subscribers to access their device over the internet and remotely destroy all of the data contained on the device. For that reason, the device may only be powered in a secure environment or, if possible, started in "airplane mode," which disables access to the network. Unlike typical computers, many cellular telephones do not have hard drives or hard drive equivalents and store information in volatile memory within the device or in memory cards inserted into the device. Current technology provides some solutions for acquiring some of the data stored in some cellular telephone models using forensic hardware and software. Even if some of the stored information on the device may be acquired forensically, not all of the data subject to seizure may be so acquired. For devices that are not subject to forensic data acquisition or that have potentially relevant data stored that is not subject to such acquisition, the examiner must inspect the device manually and record the process and the results using digital photography. This process is time and labor intensive and may take weeks or longer.

8. Following the issuance of this warrant, the Device will be subjected to a forensic analysis. All forensic analyses of the data contained within the telephone and its memory cards will employ search protocols directed exclusively to the identification and extraction of data within the scope of this warrant and will follow the procedures below.

9. Based on his knowledge, training, and experience, the affiant knows that electronic devices, such as smartphones, can store information for long periods of time. Similarly, items that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

10. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the

application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. The affiant knows that when an individual uses an electronic device to commit a crime, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of facilitating the criminal offense, for example, communicating or researching the crime. The electronic device is also likely to be a storage medium for evidence of crime. From his training and experience, the affiant believes that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

11. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant the affiant is applying for would permit an agent's continued seizure and subsequent review of the Device as well as the forensic examination of the Device consistent with the warrant. The examination will require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

12. Following the issuance of this warrant, an agent will seize the Device and submit the Device for a forensic extraction of the Device. Subsequently, the forensic extraction will be examined for evidence described in Attachment B. All searches and forensic analysis of the data contained within the Device and its memory cards will employ search techniques directed to the identification and extraction of data within the scope of this warrant.

13. Based on the foregoing, identifying, and extracting data subject to seizure pursuant to this warrant may require a range of data analysis techniques, including manual

review, and, consequently, may take weeks or months. The personnel conducting the identification and extraction of data will complete the analysis within one-hundred twenty (120) days, absent further application to this court.

14. In searching digital data stored on digital devices, law enforcement personnel executing this search warrant will employ the following procedure:

- a. Law enforcement personnel or other individuals assisting law enforcement personnel will complete the search as soon as is practicable but not to exceed 120 days from the date of execution of this warrant. If additional time is needed, the government may seek an extension of this time period from the Court within the original 120-day period from the date of execution of the warrant.
- b. The team searching the digital devices will do so only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.
 - i. The team may subject all of the data contained in the digital device or the forensic copy capable of containing items to be seized as specified in this warrant to the protocols to determine whether the digital device and any data falls within the items to be seized as set forth herein. The team searching the digital device may also search for and attempt to recover “deleted,” “hidden,” or encrypted data to determine, pursuant to the protocols, whether the data falls within the list of items to be seized as set forth herein.
 - ii. These search protocols also may include the use of tools to exclude normal operating system files and standard third-party software that do not need to be searched.
- c. When searching a digital device pursuant to the specific search protocols selected, the team searching the digital device shall make and retain notes regarding how the search was conducted pursuant to the selected protocols.
- d. If the team searching a digital device pursuant to the selected protocols encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that digital device pending further order of Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.
- e. At the conclusion of the search of the digital devices, any digital device

determined to be itself an instrumentality of the offense(s) and all the data thereon shall be retained by the government until further order of court or one year after the conclusion of the criminal case/investigation.

- f. Notwithstanding, after the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized in this warrant on any retained digital devices or digital data absent further order of court.
- g. If the search team determines that a digital device is not an instrumentality of any offense under investigation and does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will as soon as practicable return the digital device and delete or destroy all the forensic copies thereof.
- h. If the search determines that the digital device or the forensic copy is not an instrumentality of the offense but does contain data falling within the list of the items to be seized pursuant to this warrant, the government either (i) within the time period authorized by the Court for completing the search, return to the Court for an order authorizing retention of the digital device and forensic copy; or (ii) retain only a copy of the data found to fall within the list of the items to be seized pursuant to this warrant and return the digital device and delete or destroy all the forensic copies thereof.

SUMMARY OF PROBABLE CAUSE

15. Based on the facts known in this investigation, I submit that Warren Jones Crazybull (CRAZYBULL) called Mar-a-Lago on July 31, 2024. He threatened to kill former President Donald J. Trump. (Exhibit A). Law enforcement found a Facebook page that appears to belong to CRAZYBULL. On this Facebook page, there was a publicly posted video of CRAZYBULL making comments regarding violence towards Former President Trump. (Exhibit B). CRAZYBULL also posted several written communications on his Facebook page concerning violence and anger towards Mr. Trump and Mr. John F. Kennedy (see excerpted snapshots *infra*). Law enforcement apprehended CRAZYBULL on August 1, 2024. After law enforcement provided him his *Miranda* warnings, CRAZYBULL submitted to an interview where he

admitted to posting the video. CRAZYBULL admitted to a Facebook post. CRAZYBULL claimed he posted the video and made the Facebook post to get law enforcement's attention. CRAZYBULL stated that Mr. Trump had violated treaties and thereby deprived CRAZYBULL of his land. Law enforcement seized a phone from CRAZYBULL (the phone as is identified in Attachment A). I now come before this Court to request a search warrant to review the contents of phone taken from CRAZYBULL's possession.

PROBABLE CAUSE

16. On July 31, 2024, USSS West Palm Beach Resident Office notified the USSS Protective Intelligence Division (PID)/Protective Intelligence Operations Center (PIOC) of the following incident:

- a. On July 31, 2024, Mar-a-Lago security received a phone call from number 208-406-1611. The name "Warren Jones" was displayed on the security booth phone at Mar-a-Lago. During the call several statements were made, one such statement was "Find Trump...I am coming down to Bedminster tomorrow. I am going to down him personally and kill him." Mar-a-Lago security advised the USSS that approximately eight additional phone calls making threats were received from the same phone number.

The reporting Mar-a-Lago security employee recorded a part of one of the phone calls using his personal phone as a recording device. He sent the phone call to the USSS, and it is attached to this Affidavit as Exhibit A. The reporting security employee is a civilian who is known to law enforcement. I omit his identity for privacy reasons.

17. Mar-a-Lago is a resort and National Historic Landmark in Florida. It is owned by Donald Trump. Also, Donald Trump resides there on occasion. Donald Trump was the President

of the United States. Given the calls to Mar-a-Lago threatening Mr. Trump, the USSS began an investigation.

18. To begin, USSS researched the phone number used to call in the threat. The phone number is 208-406-1611. The “208” area code is used for Idaho phones. Using open-source intelligence, the USSS PID/PIOC could not locate a record associating CRAZYBULL with the 208-406-1611 phone number.¹ Despite the phone number not being associated with CRAZYBULL according to open-source intelligence, the USSS was able to identify CRAZYBULL by the identity of “Warren Jones.” Please note, CRAZYBULL has several aliases according to law enforcement records. This includes “Warren Von Crazybull-Jones,” “Warren V Jones,” “Warren Crazybull Jones,” and “Warren Von Jones.”

19. In further researching CRAZYBULL, law enforcement found a Facebook page that appears associated with or controlled by CRAZYBULL.² I submit that this Facebook page is associated with or controlled by CRAZYBULL for at least two reasons. First, the name on the Facebook page is “Tracy Jones.” “Jones” is CRAZYBULL’s legal middle name and used in his aliases as a last name. Second, there was a video posted on the Facebook page that appears to be a self-produced narrative that contains threats to Mr. Trump. As for this video, it was posted on or about July 31, 2024. This video is included as Exhibit B. I submit that the content of the audio in Exhibit A matches, in part, the tone and content to the audio in Exhibit B. A still picture from Exhibit B appears as:

¹ This possibly indicates that the phone number and/or phone could belong to another person, that CRAZYBULL secured this phone number using non-contracted or recorded means, or that he was using a Voice-over-Internet-Protocol (VoIP) service.

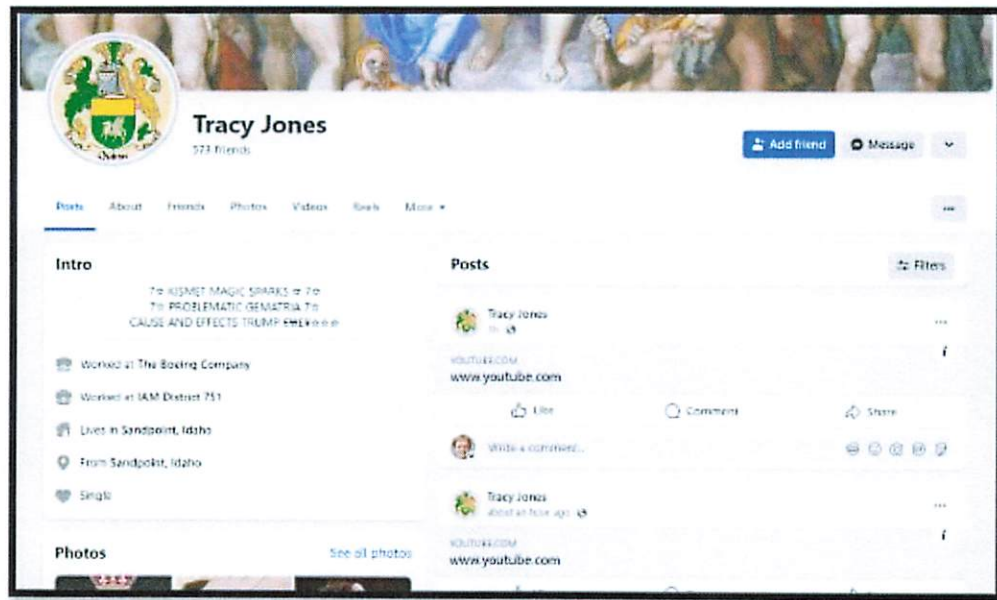
² Facebook is a social media and social networking internet-based site (and phone application) whereby people can post information.



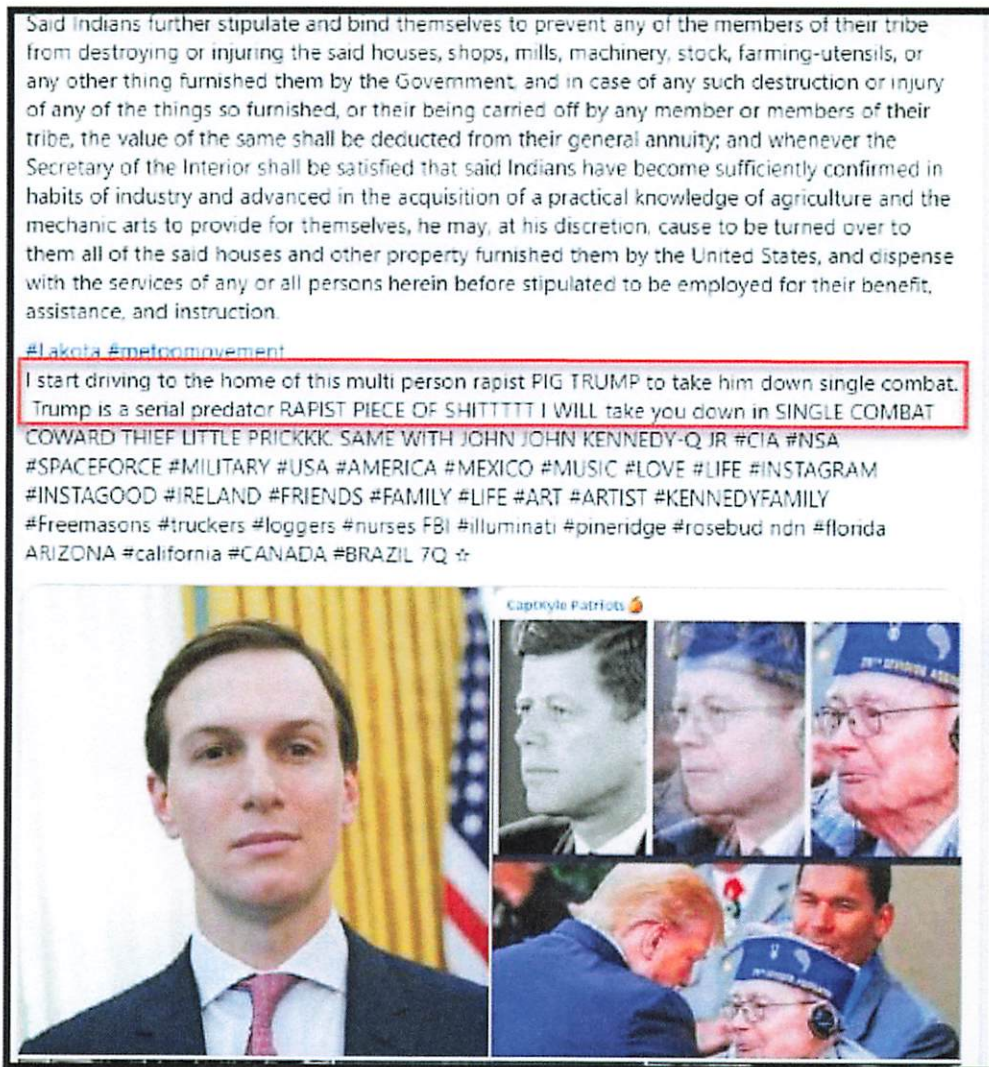
I submit that the man depicted in Attachment B is CRAZYBULL. I do so, as the image matches the Washington Department of Motor Vehicles (DMV) photo of CRAZYBULL. Law enforcement was able to find a picture of CRAZYBULL according to Washington DMV records. He appears as follows:



20. In addition to the audio communication to Mar-a-Lago and the posted video to Facebook, law enforcement discovered posts from the Facebook page bearing screenname “Tracy Jones.” The Facebook account header, when accessed by law enforcement on or about July 31, 2024, appears as follows:



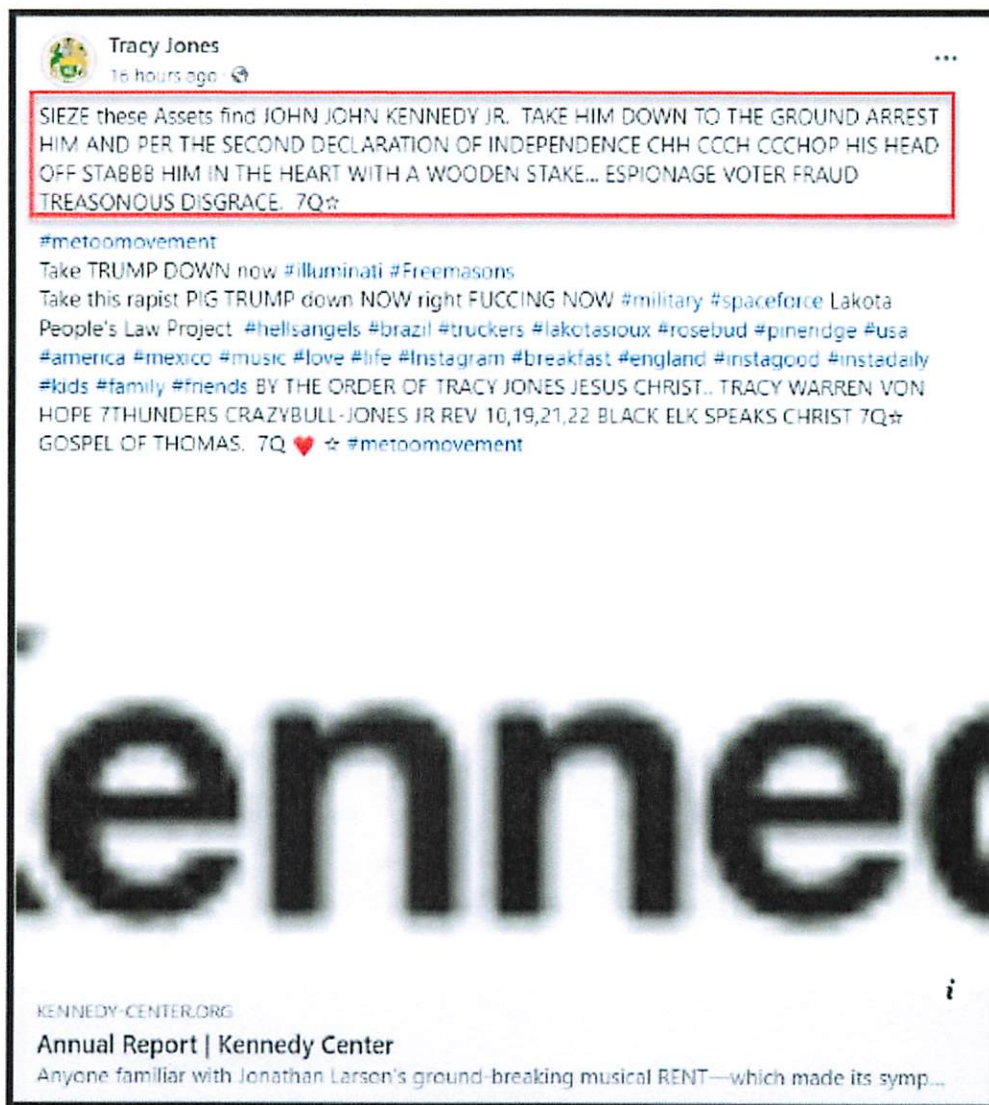
21. There were several concerning posts on this Facebook page. For example, one post stated, “I start driving to the home of this multi person rapist PIG TRUMP to take him down single combat.” This post appears as follows:



The red box was added by law enforcement. Once again, this post has similarities to the other communications from CRAZYBULL. Other posts have similar appearances. They are as follows:







The red boxes above were added by law enforcement while analyzing the Facebook page. There is a time display for the posts above (one that indicates “7 hours ago” and one that indicates “16 hours ago”). These time displays are relative to the time the posts were accessed by the viewer. To my knowledge, these posts were publicly posted on or about July 31, 2024. Facebook is an online social networking platform that can be accessed by a web browser or by a computer application on portable digital device (such as the phone identified in Attachment A).

22. Law enforcement continued the investigation. This included looking at open-source intelligence for other phone number associated with CRAZYBULL. Law enforcement found a phone number, 208-405-1611, associated with CRAZYBULL and administered by T-Mobile. Given the repeated communications and threats, USSS PID/PIOC provided an exigent request to T-Mobile for phone pings to the phone using the number 208-405-1611. A “phone ping” is the act of determining the current location of a cell phone. These phone pings placed the phone in the District of Idaho at the time the threats were posted online. The phone pings then showed that CRAZYBULL traveled into Montana on or about August 1, 2024.

23. Based on phone pings, law enforcement was able to locate CRAZYBULL. He was apprehended by law enforcement on August 1, 2024. After his arrest, he was provided his *Miranda* warnings. CRAZYBULL waived his *Miranda* warnings in writing and agreed to an interview with a USSS agent. CRAZYBULL relayed the following:

- a. CRAZYBULL stated he was currently living out of his vehicle.
- b. CRAZYBULL stated he was Chief of the Rosebud tribe and is royalty.
- c. CRAZYBULL stated that he blames former Presidents Trump and John F. Kennedy for broken treaties that resulted in the loss of his land.
- d. When asked about the video he posted (Exhibit B), CRAZYBULL stated he posted the video to get law enforcement’s attention.
- e. Throughout the interview, CRAZYBULL repeatedly said he would not let Trump become president again.
- f. CRAZYBULL stated he would not attempt to kill Former President Trump.
- g. CRAZYBULL stated that he did not have any special skills or training and had never served in the military.
- h. CRAZYBULL stated that he did not own a firearm and had not fired a weapon since childhood.

- i. CRAZYBULL has been admitted for psychiatric care in the past but could not remember the date(s) of admission.
- j. CRAZYBULL stated that he was not taking any psychiatric medication at the time of interview.

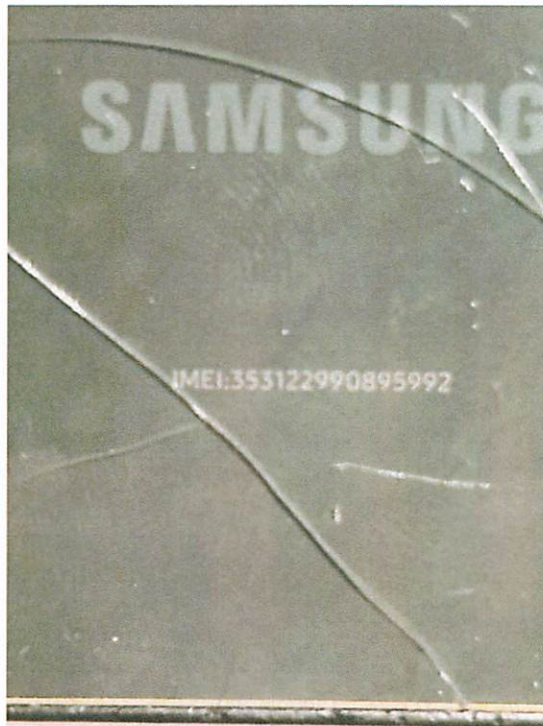
Additionally, CRAZYBULL was asked about his posting indicating he was going to drive to Bedminster (this is relevant to the USSS, as the Trump National Golf Club Bedminster is located there. Former President Trump uses this location as one of his residences). CRAZYBULL stated he posted about Bedminster to get law enforcement's attention. During the interview, CRAZYBULL appeared as if his thought processes were racing and confused. According to the interviewing law enforcement agent, CRAZYBULL also seemed paranoid.

24. As for this warrant, CRAZYBULL was arrested and had a cellular phone. The cell phone was located in CRAZYBULL's vehicle when he was stopped and detained by the Montana Highway Patrol (MHP). Prior to departing the scene, CRAZYBULL asked the officer for his phone so that he could call his daughter. CPT Eric Federholf (MHP) retrieved the phone from the vehicle and gave it to CRAZYBULL. The phone was taken from CRAZYBULL when he was processed into the Gallatin County Detention Center. CRAZYBULL's cell phone (the subject of this warrant) was taken by detention deputies at the Gallatin County Detention Center while he was being processed for custody purposes (to my knowledge, inmates cannot keep or bring their cell phones into the detention center). I seized the cell phone on or about 7:22 pm mountain standard time, upon conclusion of his interview with CRAZYBULL, from Gallatin County Detention Center staff. Law enforcement observed the phone and can identify it with specificity as a black Samsung Cell Phone bearing International Mobile Equipment Identity Number 353122990895992.

The phone appears as follows:



The phone has an International Mobile Equipment Identity (IMEI) number of 353122990895992, which is visible on the device, and appears as follows:



I know that the IMEI identifies the phone with specificity, as no two phones share an IMEI. The cellular phone was taken by law enforcement to Billings, Montana located at 401 N 31st St. #600, Billings, Montana 59101. It remains there, secured in law enforcement custody, pending issuance of a warrant.

25. The Device is currently in of the USSS Billings, MT Resident Agent. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the USSS.

26. Given the above, I submit there is probable cause to search the Device. The threats were issued using a digital device. CRAZYBULL, in his interview, claimed he lived out of his car. Given that the Device, as identified in Attachment A, was found on his person and he does not keep a residence (according to CRAZYBULL), I submit that it is probable this Device

was used in the criminal activity described above. It was probably used to record, post, and research knowledge necessary to communicate and issue the threat. Accordingly, I believe the items identified in Attachment B will be on the Device. Additionally, CRAZYBULL engaged in activities that indicate online research. For example, he called Mar-a-Lago. I submit it is probable he acquired this phone number from online research. Records of this would serve of evidence of the crime. Additionally, in my experience, persons who express repeated and forceful communications as CRAZYBULL did often have a period of fixation and research. Put simply, the threatening behavior and knowledge to issue the threats did not likely occur only the date the threat issued. Accordingly, I submit there is probable cause for time period exceeding the date of the issuance of the threat.

TECHNICAL TERMS

27. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. **Wireless telephone:** A wireless telephone (or mobile telephone, cellular telephone, or cell phone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and

storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets,

and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

- f. **Tablet:** A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.
- g. **IP Address:** An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- h. **Internet:** The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international

borders, even when the devices communicating with each other are in the same state.

28. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at <https://www.samsung.com>, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, tablet, PDA, GPS navigation device, and can access the internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

Respectfully Submitted,



JERRARD CARTER
Senior Special Agent
United States Secret Service

SUBSCRIBED and SWORN to before me consistent with Fed. R. Crim. P. 4.1 on this
20 day of September, 2024.



TIMOTHY J. CAVAN
United States Magistrate Judge